CLAIMS

1. A method for analyzing a network protocol stream for a security-related event, comprising:

identifying at least two states associated with the network protocol in which a first host system communicating with a second host system using the network protocol may be placed;

defining at least one valid transition between a first state of the at least two states and a second state of the at least two states;

expressing the at least one valid transition in the form of a regular expression; and

using the regular expression to analyze the network protocol stream.

2. A method for analyzing a network protocol stream as recited in claim 1, wherein using the regular expression to analyze the network protocol stream comprises compiling the regular expression into computer code.

3. A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises code in the C programming language.

4. A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises optimal computer code.

5. A method for analyzing a network protocol stream as recited in claim 2, wherein the computer code comprises nearly optimal computer code.

6. A method for analyzing a network protocol stream as recited in claim 1, wherein using the regular expression to analyze the network protocol stream comprises copying the network protocol stream to a third system and using the regular expression to analyze the network protocol steam at the third system.

7. A method for analyzing a network protocol stream as recited in claim 6, wherein the network protocol stream comprises packets of data, each packet being associated with a sequence number indicating its position relative to other packets in the protocol stream, and the third system reassembles the packets into the order indicated by the respective sequence numbers of the packets received.

8. A method for analyzing a network protocol stream as recited in claim 7, wherein a copy of the network protocol stream is maintained in the third system until analysis has been completed.

9. A method for analyzing a network protocol stream as recited in claim 7, wherein in the event the packets are received by the third system in sequence number order, a copy is maintained in the third system only of those packets comprising the portion of the network protocol currently under analysis.

10. A method for analyzing a network protocol stream as recited in claim 1, further comprising keeping track of which of the at least two states the first host system currently is in.

11. A method for analyzing a network protocol stream as recited in claim 10, further comprising changing the tracked state of the first host system from the first of the at least two states to the second of the at least two states in the event the analysis of the network protocol stream indicates the at least one valid transition has taken place.

12. A method for analyzing a network protocol stream as recited in claim 1, further comprising:

defining at least one invalid operation for the first host system in at least one of the at least two states;

expressing the at least one invalid operation as a second regular expression; and

using the second regular expression to analyze the network protocol stream.

13. A method for analyzing a network protocol stream as recited in claim 12, wherein the invalid operation may indicate that a security-related event has taken or is taking place.

14. A method for analyzing a network protocol stream as recited in claim 12, further comprising defining a further state corresponding to the invalid operation.

15. A method for analyzing a network protocol stream as recited in claim 14, further comprising:

keeping track of which state, from the set comprising the at least two states and the further state, the first host system currently is in; and

changing the state of the first host system to the further state in the event that the analysis of the network protocol stream indicates the invalid operation has taken place.

16. A method for analyzing a network protocol stream as recited in claim 15, further comprising providing, in the event that the analysis of the network protocol stream indicates the invalid operation has taken place, an indication that the invalid operation has taken place.

17. A method for analyzing a network protocol stream as recited in claim 15, further comprising discontinuing analysis of the network protocol stream once the state of the first host system has been changed to the further state.

18. A method for analyzing a network protocol stream for a security-related event, comprising:

identifying at least two valid states in which a first host system communicating with a second host system using the network protocol may be placed;

defining at least one valid transition between a first valid state of the at least two valid states and a second valid state of the at least two valid states;

expressing the at least one valid transition in the form of a first regular expression;

defining at least one invalid operation for the first host system in at least one of the at least two valid states;

expressing the at least one invalid operation as a second regular expression;

defining a further state corresponding to the invalid operation;

using the first regular expression and the second regular expression to analyze the network protocol stream, the analysis comprising providing an indication in the event the at least one invalid operation is detected.

19. A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two states associated with the network protocol, the system comprising:

a computer configured to receive and analyze the network protocol stream by processing a regular expression, the regular expression corresponding to a valid transition from a first state of at least two states to a second state of the at least two states; and

memory associated with the computer and configured to store the regular expression.

20. A system for analyzing a network protocol stream between a first host system and a second host system for a security-related event, the first host system being susceptible to being placed under the network protocol in one of at least two states associated with the network protocol, the system comprising:

means for receiving the network protocol stream; and

means for analyzing the network protocol stream by processing a regular expression, the regular expression corresponding to a valid transition from a first state of at least two states to a second state of the at least two states.

21. A computer program product for analyzing a network protocol stream, the computer program product being embodied in a computer readable medium and comprising computer instructions for:

identifying at least two states in which a first host system communicating with a second host system using the network protocol may be placed;

defining at least one valid transition between a first state of the at least two states and a second state of the at least two states;

expressing the at least one valid transition in the form of a regular expression; and

using the regular expression to analyze the network protocol stream.